UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,654	08/15/2001	Menno Anne Treffers	PHNL 000448	1920

7590 07/20/2006

Stephen B. Salal
Harter, Secrest and Emory LLC
1600 Bausch & Lomb Plaza
Rochester, NY 14604

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/930,654
Filing Date: August 15, 2001
Appellant(s): TREFFERS ET AL.

Michael J. Didas
Attorney
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5/12/2006 appealing from the Office action mailed 10/17/2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2001/0042043	SHEAR et al.	11-2001
6,226,618	DOWNS et al.	5-2001
5,892,900	GINTER et al.	4-1999
6,064,751	SMITHIES et al.	5-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 3-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shear (U.S. Patent Application Publication 2001/0042043) in view of Downs (U.S. Patent 6,226,618) and Ginter (U.S. Patent 5,892,900).

Regarding Claim 1,

Shear discloses a method for controlling distribution and use of a digital work, comprising the steps of:

a) Attaching a usage right information to the digital work, the usage right information defining one or more conditions which must be satisfied in order for a usage right of the usage right information to be exercised (Page 11, Paragraph 169);

b) Storing the digital work and the attached usage right information on a record carrier (Page 11, Paragraph 170);

d) Refusing use of the digital work if the usage right information indicates that the usage right has been exercised Page 17, Paragraph 251);

Characterized in that the method further comprises the step of:

e) Storing a hidden information in a hidden channel used for encrypting or verifying the usage right information (Pages 15-16, Paragraphs 216-220);

But does not disclose updating the attached usage right information with every use of the digital work and changing the hidden information when the usage right information has changed.

Downs, however, discloses updating the attached usage right information with every use of the digital work (Column 21, lines 42-63). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content delivery system of Downs

into the rights protection system of Shear in order to enforce the usage rights on the original copy and any new secondary copy.

Downs does not disclose changing the hidden information when the usage right information has changed.

Ginter, however, discloses changing the hidden information used for encrypting or verifying the usage right information when the usage right information has changed (Column 136, lines 37-42). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the rights protection system of Ginter into the rights protection system of Shear as modified by Downs in order to lessen the time during which each key is used, giving an attacker less ciphertext to use in an attempt to obtain the key (Column 212, lines 43-52).

Regarding Claim 11,

Claim 11 is an apparatus claim that is broader than method claim 1 and is rejected for the same reasons.

Regarding Claim 13,

Claim 13 is an apparatus claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 3,

Shear as modified by Downs and Ginter discloses the method of claim 1, in addition, Ginter discloses that the hidden information is a key used for decrypting the usage right information, wherein the changing step

includes randomly changing the key and re-encrypting the usage right information using the changed key, when the usage right information has changed (Column 136, lines 37-59).

Regarding Claim 4,

Shear as modified by Downs and Ginter discloses the method of claim 3, in addition, Ginter discloses that the previous key is destroyed after the change of the key (Column 214, lines 4-14).

Regarding Claim 5,

Shear as modified by Downs and Ginter discloses the method of claim 1, in addition, Shear discloses that the hidden channel is arranged to be not accessible by commercial reproducing devices (Page 15, Paragraph 218).

Regarding Claim 6,

Shear as modified by Downs and Ginter discloses the method of claim 5, in addition, Shear discloses that the hidden channel is generated by: storing the hidden information in deliberate errors which can be corrected again, storing the hidden information in merging bits of a runlength-limited code, controlling a polarity of predetermined runlength of a predetermined word of a runlength-limited code according to the hidden information, storing the hidden information in deliberate errors in a time-base, or storing the hidden information in a memory embedded with a disc controller (Page 15, Paragraph 218).

Regarding Claim 7,

Shear as modified by Downs and Ginter discloses the method of claim 1, in addition, Shear discloses that the attached usage right information is stored in a table together with a key information used for decrypting the digital work (Page 15, Paragraph 216).

Regarding Claim 8,

Shear as modified by Downs and Ginter discloses the method of claim 1, in addition, Shear discloses that the digital work is an audio track downloaded from the Internet, and the record carrier is a recordable optical disc, a hard disc, a magneto-optic recording device, a magnetic tape, or a memory card (Page 12, Paragraph 178).

Regarding Claim 9,

Shear as modified by Downs and Ginter discloses the method of claim 1, in addition, Downs discloses that the usage right information comprises a counter information which can be updated when the usage right has been exercised (Column 21, lines 42-63).

Regarding Claim 10,

Shear as modified by Downs and Ginter discloses the method of claim 1, in addition, Shear discloses that the record carrier has a plurality of tracks, characterized in that each track of the record carrier comprises its own usage right information and hidden information (Page 13, Paragraph 183).

Regarding Claim 12,

Shear as modified by Downs and Ginter discloses the record carrier of claim 11, in addition, Shear discloses that the record carrier is a recordable optical disc, in particular a CD or a DVD (Page 11, Paragraph 162).

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shear in view of Downs and Ginter, further in view of Smithies (U.S. Patent 6,064,751).

Shear as modified by Downs and Ginter disclose the method of claim 1, but do not disclose a checksum over a data block containing information.

Smithies, however, discloses a checksum over a data block containing information (Column 13, lines 51-63). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the checksum technique of Smithies into the rights protection system of Shear as modified by Downs and Ginter in order to ensure that the data was not decrypted, modified, and re-encrypted, thus maintaining integrity.

(10) Response to Argument

Appellant argues that claim 1 claims storing hidden information used for encrypting or verifying usage right information in a hidden channel on a record carrier. This is incorrect, as the only independent claim that claims such is claim 11. Claims 1 and 13 only require some hidden channel storing hidden information used for encrypting

or verifying the usage right information. Regarding claim 11, however, Shear teaches that the recording medium can be a writeable optical medium (such as DVD-RAM). Shear also teaches the updating of usage rights on every "use" of the digital work wherein "use" is defined as in paragraph 41 of appellant's specification: "The key-locker table KLT is re-written each time its content is changed, e.g. when the usage right is consumed." This is because Shear updates the usage rights of the content (on the copy) every time a copy is made, so as to indicate if any (and how many, if so) copies are allowed to be made from the copy, a receiving device identifier, etc. This is found in Shear, pages 17-18, paragraphs 250-254.

Appellant also argues that, in Shear, keys are hidden, but are not hidden information used for encrypting usage right information. Firstly, it is pointed out that the claims do not require such a narrow use of the hidden information being used for encrypting usage right information; the claims require that the hidden information is used for encrypting or verifying the usage right information. Shear does clearly teach that the hidden information is used for encrypting or verifying the usage right information. Page 10, paragraphs 139-140 read "In accordance with further aspects provided by the present invention, a secure 'software container' is provided that allows: Cryptographically protected encapsulation of content, rights rules, and usage controls." This means that the second container within Shear is encrypted. When using this definition and viewing the cited section (Pages 15-16, paragraphs 216-220), it is clear that the hidden keys will decrypt the encrypted key block. As seen in Figure 3, the usage right information can be within the secure container. The encrypted key block

can be inside or outside the secure container. If the encrypted key block is inside the secure container, the hidden keys will decrypt the container itself. If the encrypted key block is outside the secure container, the hidden keys will decrypt the encrypted key block, and those keys from the key block will decrypt the secure container. Both situations include the hidden information being used for encrypting or verifying the usage right information that is within the secure container.

Appellant also argues that Downs does not contemplate a record carrier as the end-user device. Shear discloses that the player itself may also store a key needed to decrypt the containers and/or content (in addition to the hidden key(s) stored on the medium) as seen in Page 10, paragraph 133: "The ability of the player to access rights managed containers and/or content may also be supported by one or more stored keys inside the player that decrypts certain encrypted keys on the medium." From here it is clear that keys which decrypt the encrypted keys can be stored both on the medium itself and on the player, requiring both (sets of) keys before allowing access to all keys within the encrypted key block, and thus access to the entire content/usage rights.

Appellant also argues that there is no motivation to combine Ginter with Shear as modified by Downs. The motivation for combining Ginter with Shear as modified by Downs is "to lessen the time during which each key is used, giving an attacker less ciphertext to use in an attempt to obtain the key". The changing of the hidden information each time the usage right information is changed, as in Shear as modified by Downs and Ginter, will prevent an attacker from overwriting a newer version of the encrypted usage rights with an older version and using such since the old key is no

longer valid and will not be used for encryption or decryption. By simply combining Ginter with Shear as modified by Downs, we acquire such a benefit, however, Ginter provides the additional motivation as described above.

Appellant also argues that Shear is directed to record carriers, so there is no reason to look at Downs or Ginter. Ginter is, indeed, discussed within Shear, teaching that portions of Ginter could be incorporated into Shear, as seen by paragraphs 332, 335, and 345 of Shear, as well as others. As one example, Shear explicitly discloses that a rights management component such as a secure node could be an SPE and/or HPE as disclosed in Ginter (Page 23, paragraph 335). Shear is directed to a content distribution and usage system in which content is created along with metadata, usage rights, etc., subsequently stored or distributed in some manner (such as an optical disk), and used. Usage comes in multiple forms from simply viewing the content to creating a copy of the content with its own usage rights, perhaps being tied to a specific player. In other words, Shear is directed towards the entire system, not just a record carrier. The addition of Downs and Ginter to Shear provides at least the stated motivations in the rights protection system of Shear.

Appellant also argues that there is no random key generation in Ginter. The key generation section of Ginter is found in Column 209, line 24 to Column 212, line 23. The cited portion (Column 136, lines 37-56) incorporates this random key generation. As seen in Column 209, lines 31-35, "Good keys are random bit strings so that every possible key in the key space is equally likely. Therefore, keys should in general be derived from a reliably random source, for example, by a cryptographically secure

pseudo-random number generator seeded from such a source." Column 209, lines 54-65 read "The preferred embodiment PPE 650 may, as mentioned above in connection with FIG. 9, includes a hardware-based random number generator 542 with the characteristics required to generate reliable random numbers. These random numbers may be used to 'seed' a cryptographically strong pseudo-random number generator (e.g., DES operated in Output Feedback Mode) for generation of additional key values derived from the random seed. In the preferred embodiment, random number generator 542 may consist of a 'noise diode' or other physically-based source of random values (e.g., radioactive decay)." In other words, Ginter does teach that the keys are random.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Jeff Popham

Conferees:

Gilberto Barron

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Matthew Smithers